DePaul College Prep

Acceptable Use Policy (AUP) for Digital Information, Communication, and Technology Resources

1. Scope and Guiding Principles

DePaul College Prep provides employees and students access to technology devices, the Internet, and data systems for educational and business purposes. This policy governs all electronic activity using school-provided technology, regardless of physical location.

- **Engagement:** Online tools must be used to increase community engagement and learning.
- **Data Protection:** The school has a legal and moral obligation to protect personal data.
- **Rights:** This policy does not limit constitutional rights to freedom of speech or protected concerted activity among employees.

2. General Usage Requirements & Network Etiquette

All use of the electronic network must support education, research, or legitimate school business. **Access is a privilege, not a right.** Users are expected to abide by the generally accepted rules of network etiquette:

- **Be prepared.** Students must bring a fully charged device to school every day
- **Be polite**. Do not become abusive in your messages to others.
- **Use appropriate language**. Do not swear or use vulgarities.
- **Do not reveal** personal addresses or telephone numbers of students or colleagues.

3. Features of Educational Platforms

The school utilizes a core suite of systems to manage instruction and operations:

- **Schoology (LMS):** Used for curriculum delivery, assignment submission, grading, and classroom communication.
- **Jamf School (MDM):** Manages device security, pushes required apps, and allows teachers to focus on student devices. *Note: Jamf does not collect personal files, photos, or browsing history.*
- **Google Workspace (G Suite):** Primary collaboration suite for Docs, Sheets, Slides, and Drive storage.
- **Apple Classroom:** Allows teachers to view students' screens in real time, launch apps, and lock screens for assessments.
- **Microsoft Office 365:** Provides access to professional tools, including Word, Excel, PowerPoint, and Outlook, for business and college-readiness.

4. Internet Safety & Email Use

- **Safety:** Users shall not access harmful or "adult" material. The school uses filtering software to block obscene material.
- **Email:** School-issued email accounts are the only authorized accounts for school-related

communication. They must be used professionally and are subject to monitoring.
- **Disclosure:** Students must not agree to meet someone they "met" online without parental permission.

5. Generative Artificial Intelligence (AI) Policy

- **Academic Integrity:** Students may only use Generative AI (e.g., ChatGPT, Gemini) when explicitly authorized by a teacher for a specific assignment.
- **Disclosure:** Any use of AI in the creation of school work must be cited or disclosed.
- **Prohibited Use:** Using AI to create "deepfake" media or to bypass original thought is strictly prohibited.

6. Security & Vandalism

- **Security:** If you identify a security problem on the network, you must notify a teacher or the IT Department immediately. Do not demonstrate the problem to other users. Do not use another individual's account without written permission.
- **Vandalism:** Vandalism is defined as any malicious attempt to harm or destroy another user's data or the school network. This includes, but is not limited to, uploading or creating computer viruses. Vandalism will result in the cancellation of privileges and disciplinary action.

7. Unacceptable Use and Prohibitions

The following actions are strictly prohibited:

- **VPNs:** Use of Virtual Private Networks to bypass school filters.
- **Copyright Law:** Unauthorized downloading, copying, or distributing of copyrighted materials is illegal.
- **Privacy Violations:** Recording or photographing individuals without their explicit consent. iPads and other recording devices may never be used in bathrooms or locker rooms
- **Cyberbullying:** Harassing, threatening, or "doxing" any member of the community.
- **Unauthorized Airdropping:** Sending files without faculty approval.
- **Legal Reporting:** Messages related to or supporting illegal activities may be reported to the appropriate authorities.

8. No Warranties & Indemnification

- **No Warranties:** DePaul College Prep makes no warranties of any kind, whether express or implied, regarding the service it provides. The school will not be responsible for any damages the user suffers, including loss of data or service interruptions.
- **Indemnification:** The user agrees to indemnify DePaul College Prep for any losses, costs, or damages, including reasonable attorneys' fees, incurred by the school relating to or arising out of any violation of this policy.

9. Legal Compliance (CIPA)

In compliance with the **Children's Internet Protection Act (CIPA)**, DePaul College Prep employs:

- **Meraki Firewall:** Advanced content filtering.
- **Active Monitoring:** Automated safety alerts via **Gaggle** and **Managed Methods**.
- **Digital Citizenship:** Mandatory instruction on safe and ethical online behavior.

Legal References:

- Children's Internet Protection Act (CIPA), 47 U.S.C. §254.
- No Child Left Behind / ESSA.
- Illinois Criminal Code, 720 ILCS 135/0.01.